

Notice of Allowability

Application No.

09/931,004

Examiner

Longbit Chai

Applicant(s)

KWAN, NANG KON

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 12/19/2005.
2. ☒ The allowed claim(s) is/are 1,2,4,5,7,9,10,18,28 and 33.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 12/19/2005.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

CEL
Primary Examiner
12/21/05

DETAILED ACTION

Claims 1 – 33 have been presented for examination. Claims 1, 5, 7, 10, 12, 14 – 17, 19, 21, 26, 28, 30 and 33 have been amended in an amendment filed 11/28/2005.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/28/2005 has been entered.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Joseph Palys (Reg. No. 46,508) on 12/19/2005.

This application has been amended as follows:

IN THE CLAIMS

Cancel claim 12 – 17, 19, 21, 25 – 27 and 30 – 32 without prejudice.

Replace claim 10 and 28 as follows.

Claim 10: A method in a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

receiving a request for a digital certificate from a user to a registration manager,
the request including an encryption key associated with the user;

providing, by the registration manager to a recovery manager, the user's
encryption key that is encrypted with a first archival key;

digitally signing, at a recovery manager, an indication of proof of archival of an
the encryption key for the user in a database;

verifying, by a the registration manager, the digitally signed indication of proof
based on a first archival key;

sending, by the registration manager to the certificate authority, a request for a
digital certificate based on the verifying; and

receiving, from the certificate authority, a digital certificate in response to the
request.

Claim 28: A computer-readable medium containing instructions for controlling a data processing system to perform a method for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, the method comprising the steps of:

receiving, at a recovery manager, a user encryption key from a registration manager that manages certificates for the user, the encryption key being signed by a first archival key;

digitally signing, by the recovery manager, an indication of proof of archival of the user's encryption key in a database under the control of an entity separate from the certificate authority, wherein the indication of proof is signed with a second archival key;

providing, by the recovery manager, the signed indication of proof to the registration manager;

verifying, by the registration manager, the digitally signed indication of proof based on the first archival key;

sending, by the registration manager, a request for a digital certificate based on the verified digitally signed indication of proof; and

receiving, by the registration manager, a digital certificate in response to the request.

Allowable Subject Matter

1. Claims 1, 2, 4, 5, 7, 9, 10, 18, 28 and 33 are allowed.
2. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claim 1 and subsequent dependent claims.

The prior arts Brisbee, alone or in combination with CSFB, fail to teach or suggest process steps and/or elements associated with a registration manager, recovery manager, and certificate authority or similar entity, as recited in the pending claims. Therefore, the CPA does not teach or suggest a system or apparatus for method in a data processing system for requesting a digital certificate from a certificate authority and archiving an encryption key outside of the certificate authority, comprising:

receiving, at a registration manager, a request from a user for a digital certificate, the request including an encryption key associated with the user;

encrypting the user's encryption key with a first archival key;

providing, by the registration manager, the user's encryption key that is encrypted with the first archival key;

storing, by a recovery manager, the encrypted user's encryption key in a database;

providing, by the recovery manager to the registration manager, an indication of proof of storing the encrypted user's encryption key, wherein the indication of proof is signed with a second archival key;

verifying, by the registration manager, the signed indication of proof based on the first archival key; and

providing, by the registration manager, the request to the certificate authority based on the verification of the signed indication of proof.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC 


Primary Examiner
AU 2131
12/21/05